SysAdmin's Notebook

SSL Public Key Pinning – Bulletin

Mozilla has introduced a new feature in the latest release of its popular web browser, Firefox Version 32. The feature is SSL Public Key Pinning and is designed to help prevent "Man in the Middle"(MITM) attacks. For those who are worried that this feature might cause issues in a FortiGate firewall protected environment, there is little reason for concern. Any incompatibility issues are slight and easily corrected.

The basic premise of Pinning is that it enables the web browser to recognize or verify a specific selection of Certificate Authorities as the correct issuers of certificates for websites that are part of the Pinning feature. For example, one of the first websites that includes this feature is Twitter. If you are using Firefox version 32 or later and you go to a Twitter website that uses SSL, Firefox not only checks to make sure that the website has an SSL certificate associated with the URL to which you connect, but it also verifies that the certificate is issued by a particular Certificate Authority that is known to issue certificates to Twitter. This prevents “Man in the Middle” attacks by malicious agents providing false certificates that give the impression that everything is safe and secure, when the certificate is not actually issued to Twitter.

There are 4 levels of Pinning you can use in Firefox version 32:

0 – Pinning is disabled.
1 – Allow User MITM (Pinning is not enforced if the trust anchor is a user inserted CA, default).
2 – Strict mode. Pinning is always enforced.
3 – Enforce test mode.

According to Mozilla’s Public Key Pinning wiki, Firefox version 32 currently includes Pinning only for Twitter and Mozilla websites. However, Firefox plans to implement Pinning on the following websites in the near future:

- Google
- Firefox
- TOR
- Dropbox
- Additional Mozilla websites
- Additional Twitter websites

Website operators interested in utilizing Firefox’s Pinning feature for their websites can visit Mozilla’s Public Key Pinning Implementation wiki for more information.

Now that we have a basic understanding of Pinning, we need to determine how it affects a Fortinet environment. Unless you are visiting one of the websites on Firefox’s “pinned” list, a Fortinet environment shouldn’t be affected at all. The point at which Pinning becomes problematic is when a Firefox user goes through a FortiGate’s firewall policy that includes SSL inspection to one of the websites on Firefox’s “pinned” list. The problem is that in order to execute deep SSL inspection, the FortiGate performs the same actions that occur during a “Man in the Middle” attack, which is exactly what Firefox’s Pinning feature is designed to prevent.

If this Pinning feature causes a conflict in your FortiGate protected environment you have a few options:

On the Firefox browser

Add certificates to the browser.

The default level setting for Pinning is: “1. Allow User MITM (Pinning is not enforced if the trust anchor is a user inserted CA, default)” This means that if the certificate is added to Firefox’s list of trusted certificates you should be good to go.

Disable Pinning in Firefox version 32 and later

Disable the Pinning feature in Firefox version 32 and later. While it is enabled by default, it can be disabled. If you wish, it can also be made stricter.

To change the Pinning level:

1. In the Firefox browser, enter the URL: `about:config`
2. Scroll down to the Preference Name: `security.cert_pinning.enforcement_level`
3. Double click the row with the value you intend to change.
4. Change the Level to: `0`

   Note: Changing the Level to `0` disables Pinning. Change the Level to `2` to make the feature stricter.
5. Select OK.

On the FortiGate firewall

Configure FortiGate firewall policies to use SSL Certificate Inspection

When setting up an SSL/SSH inspection profile, two Inspection method options are available. You can either use ‘Full SSL Inspection’ or ‘SSL Certificate Inspection’. The ‘SSL Certificate Inspection’ method looks only at the header of the packets to make sure that there is a proper certificate included and does not actually decrypt the contents of the packets. Decrypting and re-encrypting the contents of the packets triggers a untrusted website warning from Firefox because it receives a FortiGate certificate, rather than the original. This level of inspection ensures that you are connected to the correct website, but will not inspect the content for malware or other content that you may be filtering.

Configure additional FortiGate firewall policies

Create a policy for websites in the “pinned” list and do not implement deep inspection on that traffic. This would mean using either ‘SSL Certificate Inspection’ (in FortiOS 5.2) or no SSL inspection. Depending on how seriously you wish to scan the contents of SSL traffic, you can create separate policies for websites that are affected by Pinning and use your existing policies for all other traffic. The drawback of this strategy is that there is increased administrative overhead to remain up-to-date with the changes.

Final thoughts

The Pinning feature is something relatively new to the Internet environment, so you can expect a few growing pains initially. In fact, Google’s Chrome browser has already been doing this for Google websites for some time. The difference with the Firefox implementation is that eventually a significantly larger number of websites will be involved. Pinning is fairly straightforward, and since Fortinet has made accommodations for the possible inconveniences associated with SSL deep scanning in FortiOS 5.2, this feature can be used without any overt drawbacks.